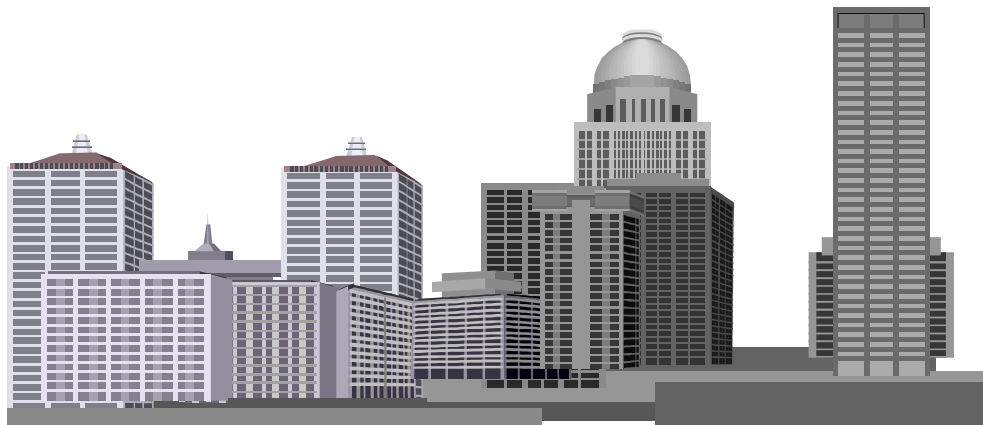


Metro Archives Newsletter



March-April, 2012

Hacker Activity Could Mean Computer Outages in 2012

Inside this issue:

<i>Hackers & Potential Computer Outages.</i>	1
<i>Federal Records Management Improvement Plans</i>	1
<i>Government Passwords and IT Security Dangers</i>	2
<i>Searching for Your Roots in City Directories</i>	2
<i>Keeping the Internet Open; A Whitehouse Promise</i>	3
<i>Schedule of Upcoming Events</i>	4



According to an article in *Nextgov.com*, computer security firm McAfee predicts hackers will join forces with offline protesters in 2012 for strikes on transportation computer systems and other critical government networks. McAfee reports that its yearly assessments are meant to convince authorities and network administrators to take threats more seriously.

Dave Marcus, security research director for McAfee Labs, said. "We don't write them to be doom-sayers. It's possible to secure these types of systems. But part of that preparedness may require changing behavior."

According to the article, annual predictions released by McAfee note that anti-Wall Street protesters occupying parks in cities across the country and digital activists associated with the group Anonymous may soon operate as "cyberoccupiers."

"Think about the effectiveness if you actually shut down transportation in the place that you're sitting in at," said Marcus. "You actually take the step of taking their power offline."

According to the article, the Pentagon recently equated cyberattacks to acts of war that can warrant strikes in response, and next year, McAfee says, the U.S. military will show its cyber capabilities.

"I think governments are going to be much more up front about what kind of cyber capabilities they have," Marcus said. "It looks like, from an outsider view, that China walks all over us." War games would allow for "showing off your digital weaponry in a different kind of format, which is a safer way to intimidate without divulging actual probes," Marcus added.

Nextgov.com reported that other 2012 scenarios envision that the

"hacktivists" will increase the amount of disclosures of government officials' e-mails and other private data. And, according to McAfee, industrial supervisory control and data acquisition systems that operate power grids and water plants will be more vulnerable because they were not designed for the Internet environment.

"It's time for extensive penetration testing and emergency response planning that includes cybercomponents and networking with law enforcement at all levels," Marcus stated.

"I think most of us tend to favor self-regulation," Marcus said. "But for something as big as infrastructure, you may need the government involved." Additionally, Marcus noted that officials should provide companies with resources and guidance, not just penalize them.

*ARMA International
Washington Policy Brief, Jan 2012*

Obama Demands Agencies Report Plans for Improving Federal Records Management

On Monday, November 28, 2011, President Barack Obama announced in a memorandum that agencies must deliver plans for modernizing their records management policies by late March. According to an article in the *Federal Times*, agencies must describe how they will improve or maintain their records management programs, including e-mail, social media, and other electronic communications.

The *Federal Times* reported that the memo urges officials to digitize records whenever possible. Obama explained that the greater use of electronic communications has "radically increased" the information that agencies must manage, but that technology "can make these records less burdensome to manage and easier to use and share."

Additionally, the memo orders agencies to explain how they will use cloud-based services and storage solutions, as well as to point out any holes or provisions in existing laws or regulations that get in the way of better management.

Continued on page 2

DON'T FORGET TO SIGN UP FOR RECORDS MANAGEMENT & ARCHIVES TRAINING — THRU METRO UNIVERSITY ON MARCH 15

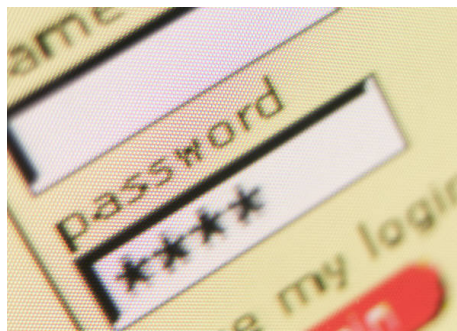
Personal Use of Work Passwords Expose Government IT Systems

The Arizona Department of Public Safety (Arizona DPS) is urging workers to stop using agency passwords on non-work websites. The warning followed an attack in late December by the group Anonymous in which it leaked the passwords and credit card data of federal subscribers to intelligence publisher Stratfor.

According to an article in *Nextgov.com*, Arizona DPS spokesman Carrick Cook stated that Anonymous allegedly unlocked state government systems by stealing and reusing the passwords officers used to access their personal e-mail accounts and non-work websites.

Former Anonymous member Jennifer Emick said some of the functioning passwords came from explicit websites, where police had registered using their government e-mail addresses and government passwords. Hackers were able to use those user names and passwords to sign on to the Arizona DPS databases.

Cook, on the other hand, said he didn't know all the details, but one gateway for hackers was the officers' personal web mail accounts. Cook noted that some police had forwarded work e-mails, which displayed their computer



credentials, to their personal accounts. "Once they [the hackers] got into the work email system – into the mainframe – they could get into the server," Cook said.

According to the article, Cook stated that

police were instructed to create stronger passwords that contain a certain number of characters, letters, and numbers. Additionally, officers are prohibited from using any personal account passwords as government logins and must contact the system administrator or enter a current password to change their codes.

Nextgov.com reported that the FBI has arrested roughly 20 "cyber crooks" aligned with Anonymous over the last year and that the current attack was a result of the group's anger over Arizona's immigration policies.

The article noted that Stratfor's investigation and coordination with law enforcement is ongoing. Chief Executive Officer George Friedman wrote the following on the company's Facebook page: "We are diligently investigating the extent to which subscriber information may have been obtained."

Searching for "Roots" in City Directories

Generally a city directory will contain an alphabetical list of its citizens, listing the names of the heads of households, their addresses, and occupational information. Sometimes the wife's name will be listed in parentheses or italics following the husband's. Often, dates of deaths of individuals listed in the previous year's directory are listed as well as the names of partners of firms, and when possible, the forwarding addresses or post offices of people who moved to another town. In addition to the alphabetical portion, a city directory may also contain a business directory, street directory, governmental directory, and listings



of town officers, schools, societies, churches, post offices, and other miscellaneous matters of general and local interest. There are usually several parts to a city directory. The section of most interest to the genealogist, of course, is the alphabetical listing of names, for it is there that you may find your ancestor.

Whenever you use a directory, however, it is important to refer to the page showing abbreviations used in the alphabetical section of the directory, usually following the name in each entry. Some abbreviations are quite common, such as *h* for home or *r*, indicating residence. There may even be a subtle distinction between *r* for residents who are related to the homeowner and *b* for boarders who are not related.

Some city directories list adult children who lived with their parents but were working or going to school. Look for persons of the same surname residing at the same address. If analyzed and interpreted properly, these annual directories can tell you (by implication) which children belong to which household, when they married and started families of their own, and when they established themselves in business. In cases where specific occupation is given, you can search records pertinent to that occupation.

At Louisville Metro Archives and Records Center, we house most Louisville city directories from 1832 to the year 2000. Visit our library M-F between 8:00-5:00. We are located at 635 Industry Rd (corner of 7th and Industry). Call (502) 574-2554 if you have any questions.

Improving Federal Records Management *(cont'd from page 1)*

According to the article, Obama noted that the Office of Management and Budget (OMB), the National Archives and Records Administration, and the Justice Department will use the reports to "create a government wide records management framework that is more efficient, maintains accountability by documenting agency actions and promotes appropriate public access to records."

Specifically, according to the White House

press release on the initiative, this guidance will come in the form of a Records Management Directive from the OMB director and the U.S. national archivist.

In a joint statement, watchdog groups OpenTheGovernment.org and Citizens for Responsibility and Ethics in Washington stated that 95% of agencies reported last year that they were at risk of losing electronic records. Obama's memo "puts in place a structure to

begin addressing the problem" they said.

"We look forward to working with the administration on this initiative – which is essential to accountable government – and will be following its implementation closely to make sure the resources of funds, attention and personnel are put in place to ensure its success," said Patrice McDermott, executive director of OpenTheGovernment.org.

ARMA International Internet Article

White House Promises to Keep Internet Open

The National Journal reported that following the recent backlash against pending online privacy legislation, the White House has made it clear that it will oppose any legislation meant to crack down on digital theft and counterfeiting that would diminish the openness of the Internet.

"While we believe that online piracy by foreign websites is a serious problem that requires a serious legislative response, we will not support legislation that reduces freedom of expression, increases cyber security risk, or undermines the dynamic, innovative global Internet," said a statement posted on January 14 by the Obama administration's top technology officials.

"Any effort to combat online piracy must guard against the risk of online censorship of lawful activity and must not inhibit innovation by our dynamic businesses large and small," the statement said.

According to the article, the posting by Victoria Espinel, intellectual property enforcement coordinator at the Office of Management and Budget, Aneesh Chopra, chief U.S. technology officer, and Howard Schmidt, cyber security coordinator for the White House national security team, was a response to online petitions of more than 52,000 signatures that urge the president to block any efforts by Congress to regulate the Internet and veto any bills, including the Stop Online Piracy Act (SOPA) moving through the House of Representatives.

The article noted that the Internet bills have generated a debate both online and in the business world about balancing openness on the Internet with the need to protect both cyber security and intellectual property rights. U.S. Chamber of Commerce President Thomas Donohue pledged to work with all sides in the debate to broker a compromise.

"We knew this would be a difficult issue," Donohue said at a news conference on January 12. "We believe that there are serious objections and legitimate ones that have been raised by some of our friends in the Internet business and we're working very, very

hard to get those resolved."

The White House technology team said the issues are not just matters for Congress to address through legislation. "We expect and encourage all private parties, including both content creators and Internet platform providers working together, to adopt voluntary measures and best practices to reduce online piracy," the statement said.

According to the article, in order to minimize the risks to innovation and openness, the White House officials said, "new legislation must be narrowly targeted only at sites beyond the reach of current U.S. law, cover activity clearly prohibited under existing U.S. laws, and be effectively tailored, with strong due process and focused on criminal activity."

Additionally, they have stressed that efforts to combat piracy must not undermine security or "the underlying architecture of the Internet."

"Proposed laws must not tamper with the technical architecture of the Internet through manipulation of the Domain Name System (DNS), a foundation of Internet security. Our analysis of the DNS filtering provisions in some proposed legislation suggests that they pose a real risk to cyber security and yet leave contraband goods and services accessible online," the statement said.

House Judiciary Chairman Lamar Smith (R-Texas) said in a statement that he has already taken action on that issue.

"Yesterday, I announced that I will remove the DNS blocking provision from the Stop Online Piracy Act so that the Committee can further examine and study the issues surrounding this provision," Smith said.

The National Journal reported that the White House statement emphasized that steps must be taken to strengthen protection of intellectual property.

"Let us be clear – online piracy is a real problem that harms the American

economy, threatens jobs for significant numbers of middle class workers and hurts some of our nation's most creative and innovative companies and entrepreneurs. It harms everyone from struggling artists to production crews, and from startup social media companies to large movie studios. "While we are strongly committed to the vigorous enforcement of intellectual property rights, existing tools are not strong enough to root out the worst online pirates beyond our borders. That is why the Administration calls on all sides to work together to pass sound legislation this year that provides prosecutors and rights holders new legal tools to combat online piracy originating beyond U.S. borders while staying true to the principles outlined above in this response. We should never let criminals hide behind a hollow embrace of legitimate American values," the White House officials wrote.

According to the article, the two groups that have opposed provisions of SOPA and the Senate's Protect Intellectual Property Act, also known as PIPA, issued statements on Saturday responding to the White House posting.


"We appreciate the Administration's recognition that our ability to innovate, invest, and grow the economy is dependent upon keeping the Internet open and free," said Markham Erickson, executive director of the NetCoalition that represents Google, Yahoo, and other Internet companies.

"The White House has made a valuable contribution to the ongoing debate over the Stop Online Piracy Act (SOPA) in the House and the Protect Intellectual Property Act (PIPA) in the Senate," said Sherwin Siy, deputy legal director of the advocacy group Public Knowledge. "The statement ... affirms the message that legislation tampering with the Domain Name System (DNS), one of the fundamental building blocks of the Internet, poses real risks to the security and stability of the Internet," Siy continued.


ARMA International
Washington Policy Brief, February 2012

Upcoming Events...

March 2012

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15 RIM Training Metro U	16	17
18	19	20 SPRING 	21	22	23	24
25	26	27	28	29	30	31

April 2012

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1 	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Please contact the Metro Archives Staff at (502) 574-2554 for details and/or additional information about any scheduled event/s.